4K−5

データハイディングにおける圧縮耐性の基礎理論

小林 誠士　小出昭夫　清水周一
日本アイ・ビー・エム (株) 東京基礎研究所

1 はじめに

データハイディング [1] では，デジタル・コンテンツに対して微小な操作を加えることにより，情報を不可視および不可聴の状態で隠して埋め込む．本稿では，この微小操作による変更分が量子化による圧縮処理の前後でどのように変化するか理論的に解析し，データハイディングの圧縮耐性について考察する．

損失のある圧縮手法である JPEG 圧縮 [2] は，DCT による周波数変換，周波数成分の量子化，エントロピー符号化など多数の操作から構成されているが，この中で情報の損失をもたらすのは，周波数成分の丸め込み操作による量子化である．したがって，データハイディングにより埋め込んだ情報の，JPEG 圧縮に対する耐性を考察するためには，微小変更量の量子化操作による変化について考察すれば良い．

2 量子化操作の影響

埋め込み情報の抽出では，JPEG 画像から DCT 周波数変換の単位である 8x8 画素サイズのブロックを N 個選択して，それぞれの同一位置の周波数成分を，以下のように加算して平均をとることにより，埋め込み操作の変更量を測定するものとする．

$$\overline{X} = \frac{1}{N}\sum_{i=0}^{N-1} X_i \tag{1}$$

ここで，各 X_iは同一周波数の成分なので，適用される量子化ステッサイズはすべて同一である．

デジタル・コンテンツの各データ要素が量子化操作による圧縮処理を施されたとき，圧縮の前後では一般に$\overline{X}$の大きさは変化する．このとき，測定された$\overline{X}$が圧縮前の大きさと大幅に異なれば，抽出処理は失敗し埋め込み情報は損なわれたことになる．一方，圧縮前後での変化がある許容範囲内であれば，圧縮の影響を受けることなく埋め込んだ情報を正しく抽出することができる． 以下では，この量子化操作の前後での$\overline{X}$の変化について考察する．

Datahiding theory: robustness to compressions
Seiji KOBAYASHI, Akio KOIDE, Shuichi SHIMIZU
IBM Japan Ltd., Tokyo Research Laboratory

まず，量子化操作後の平均値は以下のように表現できる．

$$\overline{X}^{(q)} = \frac{1}{N}\sum_{i=0}^{N-1} X_i^{(q)} \tag{2}$$

ここで，$X_i^{(q)}$は X_iをある量子化ステップ Q に基づいて変更した大きさを表している．したがって，ガウス記号 $[x]$ を用いると以下の関係式が成立する．

$$\frac{X_i^{(q)}}{Q} = \left[\frac{X_i}{Q} + 1/2\right] \tag{3}$$

次に，量子化操作前後での差$\overline{D}$を以下のように定義する．

$$\overline{D} = \overline{X} - \overline{X}^{(q)} \tag{4}$$

$$= \frac{1}{N}\sum_{i=0}^{N-1}(X_i - X_i^{(q)}) \tag{5}$$

ここで，$D_i = X_i - X_i^{(q)}$とおくと，$X_i^{(q)}$の定義により，$-Q/2 \le D_i < Q/2$となる．さて，X_iの分布が一様であると仮定すると，D_iの期待値 $E(D_i)$ および分散 $V(D_i)$ は i に無関係に，それぞれ以下のようになる．

$$E(D_i) = \frac{1}{Q}\int_{-\frac{Q}{2}}^{\frac{Q}{2}} t\,dt = 0 \tag{6}$$

$$V(D_i) = \frac{1}{Q}\int_{-\frac{Q}{2}}^{\frac{Q}{2}} t^2\,dt = \frac{Q^2}{12} \tag{7}$$

したがって，D_iの N平均である$\overline{D}$の期待値 $E(\overline{D})$ および分散 $V(\overline{D})$ は，$m_i = E(D_i)$，$\sigma_i^2 = V(D_i)$ とおくと，それぞれ以下のようになる．

$$E(\overline{D}) = \frac{1}{N}\sum_{i=0}^{N-1} m_i = 0 \tag{8}$$

$$V(\overline{D}) = \frac{1}{N^2}\sum_{i=0}^{N-1} \sigma_i^2 = \frac{Q^2}{12N} \tag{9}$$

ここで，$\overline{D}$は，サンプル数 Nが十分大きければ D_iの分布に依らず平均 0，分散 $Q^2/(12N)$ の正規分布へと漸近する（中心極限定理）．例えば，二項分布の場合，Nが 30 ほどであれば正規分布に近似できる．

3 量子化圧縮に対する耐性

サンプル数Nが十分に大きく，$\overline{D}$が平均0，分散$\sigma'^2 = Q^2/(12N)$の，以下に示す正規分布にしたがうとすれば，

$$\phi(\overline{D}) = \frac{1}{\sqrt{2\pi\sigma'}} e^{-\frac{\overline{D}^2}{2\sigma'^2}} \tag{10}$$

Dがある許容範囲$[-T/2, T/2]$に入らない，すなわち判定を誤る確率$F(T)$は以下のようになる．

$$F(T) = 1 - \int_{-T/2}^{T/2} \phi(t)dt \tag{11}$$

上記の関係により，誤り率$F(T)$を例えば10^{-3}に抑えるためには，以下の条件を満足すれば良いことがわかる．

$$\frac{T}{Q} = \frac{1.7}{\sqrt{N}} \tag{12}$$

上式から，ある誤り率のもとでは，許容範囲Tは量子化ステップQに比例することがわかる．したがって，圧縮率を高める，すなわちQを大きくするなら許容範囲Tも広くする必要がある．一方，許容範囲Tが固定で，圧縮率を高めていくときには，サンプル数Nを増やす必要がある．例えば，サンプル数$N = 50$，量子化ステップ数$Q = 10$のとき，許容範囲Tを±2とすれば，誤り率は10^{-3}以内に抑えられると予測できる．

4 実験および結果

実験として，サンプル画像をベースライン方式のJPEG圧縮により圧縮し，8 × 8 画素ブロック内の特定周波数のDCT係数値X_iを固定ブロック数N集めた平均値の変化$\overline{D}$を圧縮前後において測定し，その平均値および標準偏差を算出した．ここで，X_iとしては，JPEGジグザグスキャン[2]順で7番目のDCT係数値を，またサンプル画像としては，768×512画素、24bitのフルカラーの自然画像を用いた．また，実験では，$N = 50$の互いに異なる1000系列を用いることで$\overline{D}$の平均値および標準偏差を算出している．表1に，4種類の量子化ステップサイズについて，3種類の画像サンプルを用いたときの実測値をもとに$\overline{D}$の平均値および標準偏差を示す．それぞれ，上段が平均値，下段がその標準偏差を示している．また，理論値として，$N = 50$のときの式(9)から求められる標準偏差を示した．

5 まとめ

本稿では，JPEG圧縮を用い，量子化操作の前後におけるN個の周波数成分の変化量の平均$\overline{D}$が，期待値0を中心に分散$Q^2/\sqrt{12N}$のゆらぎをもって分布することを述べ，この予測が実測の結果と合致することを示した．

表 1: $\overline{D}$の平均値および分散値 ($N = 50$)

画像	量子化ステップサイズ			
	5	10	15	20
1	-0.003560	0.021540	0.018229	-0.002260
	0.192113	0.378926	0.506185	0.640755
2	-0.011000	-0.014700	-0.031700	-0.119700
	0.187148	0.340476	0.449357	0.568439
3	0.006400	0.040400	0.046200	-0.056000
	0.194099	0.381301	0.520925	0.651796
$Q/\sqrt{12N}$	0.204124	0.408248	0.612372	0.816497

参考文献

[1] 森本典繁,清水周一,小林誠士:"データハイディング技術", ITE Technical Report Vol.21 No.31, 1997

[2] ISO/IEC 10918-1, "Information technology - Digital Compression and Coding of Continuous-tone Still Images"

[3] ISO/IEC 13818-2, "Information technology - Generic coding of moving picutres and associated audio information part-2:video"

[4] P1180/D2,"IEEE Standard Board Draft Standard Specification for the Implementation of 8×8 Inverse Discrete Cosine Tranceform", 1990